

	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments	Error Definition	Errors
1	BRS	L7	375	certificate\$1 and (encrypt\$3 near3 message\$1) and (sign\$3 near3 message\$1) and (encrypt\$3 near3 (session adj key))	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:15			
2	BRS	L8	121	L7 and @ad<"20000728"	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:28	Rev'd kwic/im ages		
3	BRS	L6	1214	certificate\$1 and (encrypt\$3 near3 message\$1) and (sign\$3 near3 message\$1)	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:40			
4	BRS	L9	31	(unsigned adj integer) with (four adj byte\$1)	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:28	REV'd kwic/im ages		

5	BRS	L10	11	L9 and @ad<"20000728"	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:33			
---	-----	-----	----	-----------------------	--	----------------------	--	--	--

	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments	Error Definition	Errors
6	BRS	L12	12	certificate\$1 and (version with (additional adj field\$1))	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:46	Rev'd kwic/im ages		
7	BRS	L13	9	certificate\$1 and ((subject or subscriber) with issuer with (two adj byte\$1))	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:49			
8	BRS	L14	10	certificate\$1 and (ASCII with (validity or expiration))	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 09:54	Rev'd kwic/im ages		
9	BRS	L15	9	certificate\$1 and (ASCII same (validity or expiration) same "two digit month" same "two digit year")	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:55	REV'd kwic/im ages		

10	BRS	L16	9	(ASCII same (validity or expiration) same "two digit month" same "two digit year")	US- PGPUB ; USPAT ; EPO; JPO; DERWE NT; IBM_T DB	2004/12/2 1 08:55			
----	-----	-----	---	--	--	----------------------	--	--	--

	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments	Error Definition	Errors
11	BRS	L17	2	"6766450".pn.	US-PGPUB; USPAT; EPO; JPO; DERWE NT; IBM_T DB	2004/12/21 09:57			
12	BRS	L18	2	"20020107814".pn.	US-PGPUB; USPAT; EPO; JPO; DERWE NT; IBM_T DB	2004/12/21 09:58			
13	BRS	L19	1	wo-200106701-\$.did.	US-PGPUB; USPAT; EPO; JPO; DERWE NT; IBM_T DB	2004/12/21 09:59			

[Web](#) [Images](#) [Groups](#)^{New!} [News](#) [Froogle](#) [more »](#)[Advanced Search](#)
[Preferences](#)

Tip: Try removing quotes from your search to get more results.

Your search - **"x 509 certificate" "without date"** - did not match any documents.

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Sponsored Links

X.509 Certificate

Secure and Protect Your Online Code
Learn More about Content Signing
<http://www.verisign.com>

Find Certificate

We have what you're looking for.
Certificate & much more!
www.eWoss.com

[See your message here...](#)

Also, you can try [Google Answers](#) for expert help with your search.

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google

Set	Items	Description
S1	98540	CERTIFICAT? OR DIGITAL()SIGNATURE?
S2	670980	EXPIR? OR DATESTAMP? OR DATE OR DATING OR VALIDITY
S3	382069	TAG OR FLAG OR INDICATOR? OR TAGS OR FLAGS OR BYTE
S4	2629	S1 AND S2
S5	50	S3 AND S4
S6	2925	(WITHOUT OR SUBSTITUT? OR LACK? OR REPLAC?) (3N)S2
S7	18	S1 AND S6
S8	18	S7 NOT S5
S9	326	S1(3N)S2
S10	10	S1 AND (UNSIGNED()INTEGER? OR ASCII OR FOUR()BYTE)
S11	127	S2 AND (UNSIGNED()INTEGER? OR ASCII OR FOUR()BYTE)
S12	78	S5 OR S7 OR S10
S13	65	RD (unique items)
S14	46	S13 NOT PY>2001
S15	42	S14 NOT PY>2000
S16	42	S15 NOT PD=20000728:20020728
S17	42	S16 NOT PD=20020728:20041221
S18	985	DIGITAL()CERTIFICATE?
S19	0	S2 AND S3 AND S18
S20	44	S2 AND S18
S21	43	S20 NOT S12
S22	39	RD (unique items)
S23	24	S22 NOT PY>2000
File	8: Ei Compendex(R) 1970-2004/Dec W2	
	(c) 2004 Elsevier Eng. Info. Inc.	
File	35: Dissertation Abs Online 1861-2004/Dec	
	(c) 2004 ProQuest Info&Learning	
File	202: Info. Sci. & Tech. Abs. 1966-2004/Nov 02	
	(c) 2004 EBSCO Publishing	
File	65: Inside Conferences 1993-2004/Dec W3	
	(c) 2004 BLDSC all rts. reserv.	
File	2: INSPEC 1969-2004/Dec W2	
	(c) 2004 Institution of Electrical Engineers	
File	94: JICST-EPlus 1985-2004/Nov W2	
	(c) 2004 Japan Science and Tech Corp(JST)	
File	111: TGG Natl. Newspaper Index(SM) 1979-2004/Dec 17	
	(c) 2004 The Gale Group	
File	233: Internet & Personal Comp. Abs. 1981-2003/Sep	
	(c) 2003 EBSCO Pub.	
File	6: NTIS 1964-2004/Dec W1	
	(c) 2004 NTIS, Intl Cpyrght All Rights Res	
File	144: Pascal 1973-2004/Dec W1	
	(c) 2004 INIST/CNRS	
File	434: SciSearch(R) Cited Ref Sci 1974-1989/Dec	
	(c) 1998 Inst for Sci Info	
File	34: SciSearch(R) Cited Ref Sci 1990-2004/Dec W2	
	(c) 2004 Inst for Sci Info	
File	99: Wilson Appl. Sci & Tech Abs 1983-2004/Nov	
	(c) 2004 The HW Wilson Co.	
File	95: TEME-Technology & Management 1989-2004/Jun W1	
	(c) 2004 FIZ TECHNIK	

23/5/19 (Item 10 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00525091 99WI02-003

E-commerce: digital signature technology

Zhou, Tao

Windows NT , February 1, 1999 , n42 p75-80, 5 Page(s)

ISSN: 1083-138X

Languages: English

Document Type: Articles, News & Columns

Geographic Location: United States

Describes digital signature technology and its role in electronic commerce. Explains message hashing and encryption, how public and private keys work, and two public key trust models, direct and third-party. Discusses how the third-party model uses the Certificate Authority (CA), a trustworthy organization that certifies public keys and publishes the Certificate Revocation List (CRL). Examines the use of time stamping to guarantee a document's **validity**. Reports on the functions of several software products have included digital signature functionality into their applications. Suggests how to determine the appropriate digital signature solution, including public key infrastructure (PKI) decisions and where to publish CA information. Includes diagram, one screen display, and one sidebar. (amg)

Descriptors: Electronic Commerce; **Digital Certificates** ; Security; Privacy

Set	Items	Description
S1	13999	CERTIFICAT? OR DIGITAL()SIGNATURE?
S2	50415	EXPIR? OR DATESTAMP? OR DATE OR DATING OR VALIDITY
S3	224762	TAG OR FLAG OR INDICATOR? OR TAGS OR FLAGS OR BYTE
S4	732	S1 AND S2
S5	14	S3 AND S4
S6	680	(WITHOUT OR SUBSTITUT? OR LACK? OR REPLAC?) (3N)S2
S7	8	S1 AND S6
S8	8	S7 NOT S5
S9	238	S1(3N)S2
S10	117	S9 AND IC=(G06F-017/60 OR H04L-009/00)
S11	0	S10 AND (UNSIGNED()INTEGER? OR ASCII()CHARACTER? OR FOUR()- BYTE()VALUE?)
S12	1	S1 AND (UNSIGNED()INTEGER? OR ASCII OR FOUR()BYTE)
S13	29	S2 AND (UNSIGNED()INTEGER? OR ASCII OR FOUR()BYTE)
S14	8	S13 AND IC=(G06F-017? OR H04L-009?)
S15	8	S14 NOT (S8 OR S5)
S16	2	S10 AND (X509 OR X(N)509)

File 347:JAPIO Nov 1976-2004/Aug(Updated 041203)
(c) 2004 JPO & JAPIO

File 350:Derwent WPIX 1963-2004/UD,UM &UP=200481
(c) 2004 Thomson Derwent

8/5/8 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

011332977 **Image available**

WPI Acc No: 1997-310881/199728

Related WPI Acc No: 1997-145096; 1997-272383; 1997-457062; 1998-145077;
1998-145078; 1998-145079; 1998-456569; 1999-609395; 2001-624574;
2002-643037; 2002-667520; 2003-120210; 2003-246389; 2003-254939;
2003-804791

XRPX Acc No: N97-257508

Certificate management in cryptographic system - producing string
indicating that certificate is still valid and sending it to requesting
user to validate communication

Patent Assignee: MICALI S (MICA-I)

Inventor: MICALI S

Number of Countries: 019 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9720411	A1	19970605	WO 96US18476	A	19961118	199728 B

Priority Applications (No Type Date): US 95559533 A 19951116

Cited Patents: US 5261002; US 5450493

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
-----------	------	--------	----------	--------------

WO 9720411	A1	E 34	H04L-009/00	
------------	----	------	-------------	--

Designated States (National): CA JP

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC
NL PT SE

Abstract (Basic): WO 9720411 A

The method of managing **certificates** in a communication system
having a certifying authority involves having the certifying authority
generate **certificates** by digitally signing a given piece of data. At
a later point in time, the certifying authority produces a string that
proves whether a particular **certificate** is currently valid without
and also proving the validity of at least some other **certificates**.

Preferably, the certifying authority provides the string to a third
party who can then prove to a requesting party whether the particular
certificate is currently valid **without** proving the **validity** of at
least some other **certificates**.

USE/ADVANTAGE - Facilitates management of public key **certificate**
revocation without providing users with lists of revoked **certificates**
. User receives specific information rather than large list.

Dwg.1/1

Title Terms: CERTIFY; MANAGEMENT; CRYPTOGRAPHIC; SYSTEM; PRODUCE; STRING;
INDICATE; CERTIFY; STILL; VALID; SEND; REQUEST; USER; VALID; COMMUNICATE

Derwent Class: W01

International Patent Class (Main): H04L-009/00

File Segment: EPI

5/5/11 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013913094 **Image available**
WPI Acc No: 2001-397307/200142
Related WPI Acc No: 2001-417424
XRPX Acc No: N01-292784

Public key certificate revocation method for electronic commerce,
involves embedding terminal hash value into public key certificate

Patent Assignee: SUDIA F W (SUDI-I)

Inventor: SUDIA F W

Number of Countries: 094 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200106701	A1	20010125	WO 2000US19163	A	20000714	200142 B
AU 200060970	A	20010205	AU 200060970	A	20000714	200142

Priority Applications (No Type Date): US 99168002 P 19991130; US 99143852 P
19990715; US 99147696 P 19990806; US 99149315 P 19990817; US 99154088 P
19990915

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 200106701 A1 E 76 H04L-009/30

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP
KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT
RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

AU 200060970 A H04L-009/30 Based on patent WO 200106701

Abstract (Basic): WO 200106701 A1

NOVELTY - The **certification** authority request and receives
terminal hash value (THV) corresponding to initial random value from an
independent revocation service provider entity. The THV is embedded
into public key **certificate** and private key digitally signs the
certificate. An entity requests revocation from provider which ceases
publication of valid periodic freshness **indicator** updates for the
certificate.

USE - For controlling access to data and network resource to
provide privacy and authentication of data in electronic commerce on
Internet.

ADVANTAGE - Allows user to access numerous sources of web content
such as stock market or industry research without needing to know or
remember different login IDs and password for each service because
tickets are provided in the weekly **expiration** dates.

DESCRIPTION OF DRAWING(S) - The figure shows the schematic
representation of public key **certificate** revocation method.

pp; 76 DwgNo 3/4

Title Terms: PUBLIC; KEY; CERTIFY; METHOD; ELECTRONIC; EMBED; TERMINAL;
HASH; VALUE; PUBLIC; KEY; CERTIFY

Derwent Class: T01; T05; W01

International Patent Class (Main): H04L-009/30

File Segment: EPI

8/5/5 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014822331 **Image available**

WPI Acc No: 2002-643037/200269

Related WPI Acc No: 1997-145096; 1997-272383; 1997-310881; 1997-457062;
1998-145077; 1998-145078; 1998-145079; 1998-456569; 1999-609395;
2001-624574; 2002-667520; 2003-120210; 2003-246389; 2003-254939;
2003-804791

XRPX Acc No: N02-508357

Public key certificate management method in communication system,
involves producing string which proves validity of particular
certificate without proving validity of other certificate

Patent Assignee: MICALI S (MICA-I); CORESTREET LTD (CORE-N)

Inventor: MICALI S

Number of Countries: 001 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020107814	A1	20020808	US 956038	P	19951024	200269 B
			US 95559533	A	19951116	
			US 97823354	A	19970324	
			US 99356745	A	19990719	
			US 2000483125	A	20000114	
			US 2001915180	A	20010725	
US 6766450	B2	20040720	US 956038	P	19951024	200448
			US 95559533	A	19951116	
			US 97823354	A	19970324	
			US 99356745	A	19990719	
			US 2000483125	A	20000114	
			US 2001915180	A	20010725	

Priority Applications (No Type Date): US 956038 P 19951024; US 95559533 A
19951116; US 97823354 A 19970324; US 99356745 A 19990719; US 2000483125 A
20000114; US 2001915180 A 20010725

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020107814	A1	10	G06F-017/60		Provisional application US 956038

				Cont of application US 95559533
				Cont of application US 97823354
				Cont of application US 99356745
				CIP of application US 2000483125
				Cont of patent US 5666416
				Cont of patent US 5960083
				CIP of patent US 6292893
US 6766450	B2		H04L-009/00	Provisional application US 956038
				Cont of application US 95559533
				Cont of application US 97823354
				Cont of application US 99356745
				CIP of application US 2000483125
				Cont of patent US 5666416
				Cont of patent US 5960083
				CIP of patent US 6292893

Abstract (Basic): US 20020107814 A1

NOVELTY - The **certificates** for users' public keys are produced by
a certifying authority, after digitally signing in the data. The
certifying authority produces a string which proves the current
validity of a particular **certificate**, without proving validity of
other **certificates**.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the
following:

- (1) Off-line digital signing method; and
- (2) **Digital signature** validity extension method.

USE - For managing **certificate** in communication system to certify
users' public keys.

ADVANTAGE - Facilitates management of public key **certificate**

revocation without providing users with list of revoked **certificates** .
Reduces cost for managing the **certificates** by reducing size and
number of transmissions of **certificate** revocation lists among
participants in management scheme. Improves efficiency, since the
certifying authorities provide **certificate validity** information
without requiring a trusted directory. Prevents re-signing the
certificate by providing different one-time signature scheme, thereby
improving security.

DESCRIPTION OF DRAWING(S) - The figure shows the communication
environment illustrating **certificate** management process.

pp; 10 DwgNo 1/1

Title Terms: PUBLIC; KEY; CERTIFY; MANAGEMENT; METHOD; COMMUNICATE; SYSTEM;
PRODUCE; STRING; PROVE; VALID; CERTIFY; PROVE; VALID; CERTIFY

Derwent Class: T01; W01

International Patent Class (Main): G06F-017/60; H04L-009/00

File Segment: EPI

5/5/9 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014292367 **Image available**
WPI Acc No: 2002-113069/200215
XRPX Acc No: N02-084169

Modules registering method for computer system, involves granting or denying access to module, when module is judged to comply with access requirements

Patent Assignee: STILES INVENTIONS LLC (STIL-N)
Inventor: STILES I J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6330608	B1	20011211	US 97828721	A	19970331	200215 B

Priority Applications (No Type Date): US 97828721 A 19970331

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 6330608	B1	6	G06F-013/00	

Abstract (Basic): US 6330608 B1

NOVELTY - A module loaded into a computer memory is checked for compliance with the requirements for accessing the computer system. The module is checked for **byte code validity** to determine whether the module includes the required trademarked string. If the module complies with requirement for access, access to module is granted, otherwise denied.

USE - For registering modules to control access to computer systems, software, databases.

ADVANTAGE - Enables validating a service provider for accessing the computer system to check for computer viruses, version incompatibility and omission of agreement strings. Protects the ownership rights of computer system. Recognizes the valid, registered service providers without incurring the costs and inefficiencies of **digital signature** encoding, special purpose hardware devices, proprietary interfaces.

DESCRIPTION OF DRAWING(S) - The figure shows a detailed flowchart explaining the module registering process.

pp; 6 DwgNo 2/2

Title Terms: MODULE; REGISTER; METHOD; COMPUTER; SYSTEM; ACCESS; MODULE; MODULE; JUDGEMENT; COMPLY; ACCESS; REQUIRE

Derwent Class: T01

International Patent Class (Main): G06F-013/00

File Segment: EPI